REMARKS

By the foregoing amendment, the specification and claims 14, 30, 31, 46 and 49 have been amended to correct clerical errors and to further clarify the claimed subject matter.

In the Office Action, the drawings were objected to for failing to comply with 37 C.F.R. 1.84(p)(5) for including a reference sign not mentioned in the description; claims 31 and 32 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention; claims 1-5, 17-20, and 33-36 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Number 4,214,230 to Fak et al. (hereinafter "Fak"); claims 1, 6, 7, 12, 17, 22, 23, 28, 33, 38, 39, and 44 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Number 4,223,403 to Konheim et al. (hereinafter "Konheim"); claims 8-11, 13, 24-29, 40-43, and 45 were rejected under 35 U.S.C. §103(a) as being unpatentable over Konheim; claims 16, 32, and 48 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Number 4,223,403 to Rosenow (hereinafter "Rosenow ") in view of Ford et al., "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption" (hereinafter "Ford"); claims 21 and 37 were rejected under 35 U.S.C. §103(a) as being unpatentable over Fak in view of Ford. Reconsideration of the rejections of record is respectfully requested.

With regard to the Examiner's objection to the drawings, the specification has been amended to correct a clerical error and to mention the objected to reference sign "308c" from FIG. 3.

With regard to the §112 rejections of claims 31 and 32, claim 31 has been amended to further clarify the claimed subject matter. In particular, the "processor" referred to in claim 31 is now defined such that there is no longer a lack of antecedent basis. It is respectfully submitted that claim 31, as amended, is in full compliance with §112, second paragraph, as is dependent claim 32.

With regard to the §102(b) rejections of claims 1-5 as anticipated by Fak, independent claim 1 includes the features of: providing a first set of identification data related to a first transaction type, and performing a cryptographic operation upon the first set of identification data, thereby generating a second set of identification data related to a second transaction type. Fak, however, does not disclose the claim 1 limitation of "generating a second set of data related to a second transaction type." Fak instead discloses identification data encryption which produces resultant data used for the *same* type of transaction. Accordingly, Fak fails to anticipate claim 1 or render it obvious, and it is therefore respectfully submitted that the claim is in condition for allowance. Additionally, dependent claims 2-5 contain all the limitations of claim 1, and therefore these dependent claims should also be allowed.

With regard to the §102(b) rejections of claims 17-20 and 33-36 as anticipated by Fak, independent claims 17 and 33 also include the limitation of generating a second set of identification data related to a second transaction type. The Examiner bases the rejection of claims 17-20 and 33-36 on the same grounds as the rejection of claims 1-5. As discussed above with respect to claim 1, the feature of generating a second set of data related to a second transaction type is not disclosed or even remotely suggested by Fak. Therefore Fak cannot anticipate independent claims 17 and 33. Accordingly, it is respectfully submitted that independent claims 17 and 33 and dependent claims 18-20 and 34-36 are not anticipated by Fak and should be allowed.

With regard to the §102(b) rejections of claims 1, 6, 7, 12, 17, 22, 23, 28, 33, 38, 39, and 44 as anticipated by Konheim, independent claims 1, 17, and 33 include the features of: providing a first set of identification data related to a first transaction type, and performing a cryptographic operation upon the first set of identification data, thereby generating a second set of identification data related to a second transaction type. Konheim, however, like Fak, does not disclose or remotely suggest "generating a second set of data related to a second transaction type." Although Konheim may disclose the use of cryptography on one set of data to produce another set of data, this second set of data is not "related to a second transaction type." In fact, as disclosed by Konheim, all of the cryptographic operations and resultant data are contained in the central host. (See Konheim, col. 3, l. 22-27). Not only does Konheim disclose that the second set of data is used in the same *type* of transaction, but in fact it is used in the *same transaction*. Thus independent claims 1, 17, and 33 all contain at least one limitation absent from the teachings of Konheim. Accordingly, it is respectfully submitted that these claims are not anticipated by Konheim and are in condition for allowance. Additionally, because independent claims 6, 7, 12, 22, 23, 28, 38, 39, and 44 contain all the limitations of the claims upon which they depend, it is respectfully submitted that these claims should also be allowed.

With regard to the §102(b) rejections of claims 14, 15, 30, 31, 46 and 47 as anticipated by Rosenow, independent claims 14, 30, and 46 have been amended for clarification. It is respectfully submitted that these amended claims disclose limitations which are not disclosed or suggested by Rosenow, namely generating different cryptography keys which correspond to each bank or issuer identification number. Applicant therefore requests that these claims be allowed. Additionally, because dependent claims 15, 30, and 47 contain all of the limitations of the claims upon which they depend, Applicant requests that these claims be allowed as well.

With regard to the §102(b) rejections of claims 49 and 50 as anticipated by Rosenow, independent claim 49 has been amended to clarify that the described electronic financial transaction is of a different type from the first transaction. This limitation is not disclosed in or suggested by Rosenow, and therefore Rosenow cannot anticipate claim 49 or depending claim 50. It is therefore respectfully submitted that newly amended independent claim 49 and corresponding dependent claim 50, which includes all the limitations of the claim upon which it depends, are in condition for allowance.

With regard to the §103(a) rejections of claims 8-11, 13, 24-29, 40-43 and 45, these claims include all the limitations of the claims on which they depend, namely claims 1, 17 and 39. Each of these independent claims recites the feature of generating a second set of identification data related to a second transaction type. As discussed above, this feature is not disclosed in Konheim or any other reference cited in the Office Action. Konheim discloses only a closed system which involves a single type of transaction. Therefore, because none of the cited references disclose or render obvious the feature of generating a second set of identification data related to a second transaction type, it is respectfully submitted that these claims are in condition for allowance.

With regard to the §103(a) rejections of claims 16, 32, and 48 as unpatentable over Rosenow in view of Ford, these dependent claims include all the limitations of the claims on which they depend, including amended independent claims 14, 30, and 46 which require the generation of a cryptography key which is specific to each bank or issuer and which is generated by using a key derivation key in a cryptographic operation performed on data obtained from an identification number. This method is not disclosed by Rosenow, either viewed alone or in concert with Ford. Moreover, the references cited by the Examiner do not render these stated limitations obvious. Accordingly, Applicant respectfully requests that the Examiner review these dependent claims in light of the new clarifying amendments to the claims on which they depend. It is submitted that claims 16, 32, and 48 are in condition for allowance.

With regard to the §103(a) rejections of claims 21 and 37 as unpatentable over Fak in view of Ford, these claims depend on independent claims 17 and 33, respectively, which include the limitation of generating a second set of identification data related to a second transaction type. None of the references cited by the Examiner, viewed either alone or in combination, disclose or suggest this limitation. Accordingly, Applicant respectfully requests that the Examiner review these dependent claims in light of the new clarifying amendments to the claims on which they depend. It is submitted that claims 21 and 37 are in condition for allowance.

Accordingly, in light of the foregoing, it is submitted that claims 1-50, all of the pending claims, are in condition for allowance, and favorable reconsideration of these claims is respectfully requested.

Respectfully submitted,

Robert C. Scheinfeld
PTO Reg. No. 31,300

BAKER BOTTS, L.L.P.
30 Rockefeller Plaza
New York, New York 10112-4498

Attorneys for Applicants
(212) 408-2500

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Please amend page 12 in the specification as follows:

STEP 308. If the value of the fourth Electronic-Commerce PIN generation result exceeds the value of the ATM PIN (Step 308a), concatenate a binary-coded-decimal digit of value "1" to the left of the ATM PIN (Step 308b). Otherwise lave the ATM PIN unchanged (Step 308c). Step 308 produces a fifth Electronic-Commerce PIN generation result consisting of the ATM PIN or the ATM PIN with a "1" digit concatenated to the left.

IN THE CLAIMS:

Please amend the claims as follows:

14. (Amended) A method for generating a cryptography key which corresponds to a bank or issuer identification number, comprising:

providing a key derivation key;

using the key derivation key in a cryptographic operation performed on data obtained from an identification number, thereby producing the cryptographic key.

30. (Amended) A system for generating a cryptography key which corresponds to a bank or issuer identification number, comprising:

a memory, comprising

means for storing a key derivation key; and

means for using the key derivation key in a cryptographic operation performed on data obtained from an identification number, thereby producing the cryptographic key.

31. (Amended) The system of claim 30, further comprising ~~means for receiving data wherein the processor further comprises means for generating a key-check value suitable for determining whether the data corresponds to the cryptographic key~~:

a processor, wherein the processor further comprises means for generating a key-check value suitable for determining whether the data corresponds to the cryptographic key; and

a means for receiving data.

46. (Amended) A system for generating a cryptography key which corresponds to a bank or issuer identification number, comprising:

a memory;

a processor in communication with the memory; and

a computer-readable medium in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:

storing a key derivation key in the memory;

using the key derivation key in a cryptographic operation performed on data obtained from an identification number, thereby producing the cryptographic key.

49. (Amended) A method for generating identification data for an electronic financial transaction over a communications network, comprising the steps of:

providing a first set of identification data related to a first transaction type;

performing a cryptographic operation upon the first set of identification data to generate a second set of identification data for use in conducting said electronic financial transaction which is of a different type from said first transaction.